(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 September 2004 (30.09.2004)

PCT

(10) International Publication Number
WO 2004/084464 A2

(51) International Patent Classification[7]: H04L

(21) International Application Number:
PCT/US2004/007805

(22) International Filing Date: 12 March 2004 (12.03.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/454,558 14 March 2003 (14.03.2003) US

(71) Applicant *(for all designated States except US)*: **THOMSON LICENSING S.A.** [FR/FR]; 46, Quai A. Le Gallo, F-92648 Boulogne (FR).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **ZHANG, Junbiao** [CN/US]; 20 Jenna Drive, Bridgewater, NJ 08807 (US). **MATHUR, Saurabh** [IN/US]; 4923 Quail Ridge Drive, Plainsboro, IN 08536 (US).

(74) Agents: **TRIPOLI, Joseph** et al.; c/o Thomson Licensing, Inc., Two Independence Way, Suite 200, Princeton, NJ 08540 (US).

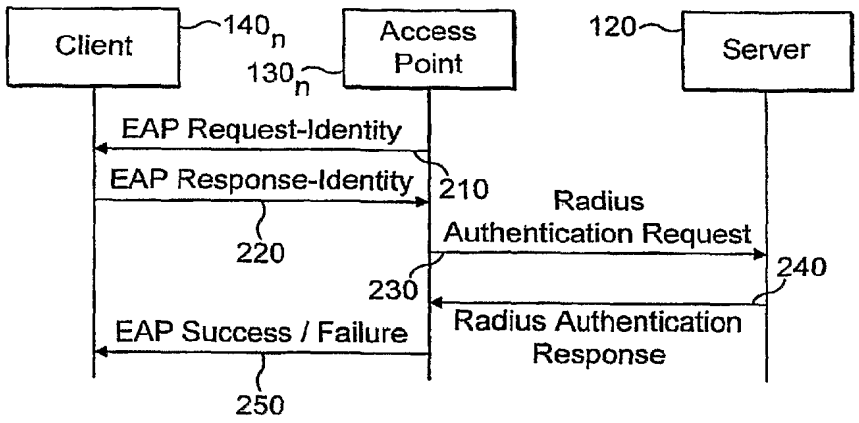
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published:**
— *without international search report and to be republished upon receipt of that report*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

(54) Title: A FLEXIBLE WLAN ACCESS POINT ARCHITECTURE CAPABLE OF ACCOMMODATING DIFFERENT USER DEVICES




(57) Abstract: The invention provides an apparatus and a method for improving the control of access by a terminal device in a WLAN environment having an access point for determining whether the device utilizes an IEEE 802.1x protocol by the access point communicating to the device, a packet, whereby if the devices utilizes a IEEE 802.1x protocol the device appropriately responds and otherwise the access point determines that the terminal device protocol does not employ a IEEE 802.1x protocol and selects an authentication mechanism compatible with the terminal device. If the device is not an IEEE 802.1x client, an IP packet filtering is configured to redirect a user HTTP request to a local server, and when the HTTP requests are thereby redirected, the HTTP server presents the terminal device with information specifically related to the browser based authentication.

WO 2004/084464 A2

# A FLEXIBLE WLAN ACCESS POINT ARCHITECTURE CAPABLE OF ACCOMMODATING DIFFERENT USER DEVICES

## RELATED APPLICATION

This application claims the benefit of U.S. Provisional Application No. 60/454,558, filed March 4, 2003, and is incorporated herein by reference.

## 1. Field of the invention

The invention provides an apparatus and a method controlling access by a user terminal to a communications network, and in particular, an apparatus and a method for controlling access by a mobile terminal to a WLAN by accommodating for each mobile terminal its particular capabilities and selecting accordingly, the optimum available authentication mechanism.

## 2. Description of Related Art

The context of the present invention is the family of wireless local area networks or (WLAN) employing the IEEE 802.1x architecture having an access point that provides access for mobile devices and to other networks, such as hard d wired local area and global networks, such as the Internet. Advancements in WLAN technology have resulted in the publicly accessible at rest stops, cafes, libraries and similar public facilities ("hot spots"). Presently, public WLANs offer mobile communication device users access to a private data network, such as a corporate intranet, or a public data network such as the Internet, peer-to-peer communication and live wireless TV broadcasting. The relatively low cost to implement and operate a public WLAN, as well as the available high bandwidth (usually in excess of 10 Megabits/second) makes the public WLAN an ideal access mechanism through which mobile wireless communications device users can exchange packets with an external entity, however as will be discussed below, such open deployment may compromise security unless adequate means for identification and authentication exists.

When a user operating a terminal incorporating the IEEE 802.1x protocol ("client terminal" or simply "IEEE 802.1x client") attempts to access a public WLAN at a hot spot, the IEEE 802.1x client terminal would begin the authentication process according to its current machine configuration. After authentication, the public WLAN opens a secure data

channel to the mobile communications device to protect the privacy of data passing between the WLAN and the device. Presently, many manufacturers of WLAN equipment have adopted the IEEE 802.1x protocol for deployed equipment. However, other devices utilizing WLAN may use other protocols such as may be provided by wired electronic privacy (WEP). Notably, the predominant authentication mechanism for WLAN utilizes the IEEE 802.1x protocol. Unfortunately, the IEEE 802.1x protocol was designed with private LAN access as its usage model. Hence, the IEEE 802.1x protocol does not provide certain convenient features necessary in a public WLAN environment. A further problem with the current predominant standard is that it requires IEEE 802.1x protocol client software installation and configuration. In addition, the IEEE 802.1x protocol does not have a sophisticated mechanism for interacting with the user. The access point can only send simple messages to the client via electronic access point (EAP) notification. This may be sufficient for an enterprise setting, but in a hot spot the access point might require that the user accept an end user license before permitting access. In some instances, the access point needs to inform the user about service charges. One solution would be to provide the access point the capability to interact with the users via the web browser interface.

Most existing WLAN hot spot wireless providers use a web browser based solution for user authentication and access control offering convenience to the user that does not require any software download on the user device. As illustrated in Figure 1, the relationships among primary entities typically involved in an authentication in a public WLAN environment are a mobile terminal (MT), a WLAN access point (AP), a local server and an authentication server (AS). In the web based solution, the user is securely authenticated through HTTPS by the AS, which in turn notifies the AP to grant access to the MT. The WLAN operator may own such an authorization server or any third party providers, such as Independent Service Providers (ISPs), pre-paid card providers or cellular operators, referred to more broadly as virtual operators. A public WLAN hot spot, therefore, should accommodate such different client and operator capabilities, based on which, the WLAN should have the ability to select different authentication mechanisms. The prior art has not sufficiently addressed means that would provide such capabilities, however, the invention described herein, provides a novel solution.

SUMMARY OF THE INVENTION

What is desired is an apparatus and a method for improving the security, or control of access by a user terminal, to a communications network, in particular the control of access by a mobile terminal to a wireless local area network.

The invention provides a method for controlling the access by a terminal device by determining the type of authentication protocol associated with the terminal device and automatically routing the authentication request to the appropriate authentication server. Specifically, the invention herein provides a method for controlling the access of a terminal device in a WLAN environment by determining whether a terminal device utilizes an IEEE 802.1x protocol, comprising the steps of an access point communicating to the mobile terminal a request to identify, and if the mobile terminal utilizes an IEEE 802.1x protocol acknowledging the request to identify, otherwise the access point determines that the mobile terminal does not employ a IEEE 802.1x protocol and therefore selects an authentication mechanism compatible with the mobile terminal.

If the terminal device is not IEEE 802.1x compliant the access point initiates a state in the access point that indicates the terminal is a non-IEEE 802.1x protocol and configures an IP packet filter and redirects a user HTTP request to a local server. The process of the present invention may also communicate from the local server to the terminal device information specifically related to a browser-based authentication. If the device utilizes the IEEE 802.1x protocol, the access point transitions to a state that indicates that the mobile terminal is IEEE 802.1x compliant and thereafter processes all further communication utilizing the IEEE 802.1x protocol. In the event that the authentication process fails, then one embodiment of the present invention initiates in the access point, a failure condition.

One embodiment of the invention for improving the security of a terminal device in a WLAN environment utilizes the access point for determining whether the device utilizes an IEEE 802.1x protocol, by having the access point communicate to the terminal device a Request-Identity EAP packet, whereby if the devices utilizes a IEEE 802.1x protocol the device responds with a Response-Identity EAP packet and otherwise the access point determines that the mobile terminal protocol does not employ a IEEE 802.1x protocol (e.g.

based on timeout) and selects an authentication mechanism compatible with the mobile terminal.

The invention for improving the security of a terminal device in a WLAN environment also includes an apparatus comprised of an access point in communication with a terminal device in a WLAN environment utilizing a means to determine whether the terminal device utilizes an IEEE 802.1x protocol and if the terminal does not utilize said protocol then the access point employs an authentication means compatible with the terminal device otherwise the access point employs an IEEE 802.1x protocol. The access point means to determine includes communicating to the terminal device a Request-Identity EAP packet and if the mobile terminal utilizes the IEEE 802.1x protocol the access receives a Response-Identity EAP packet. The access point further comprises the means to configure an IP packet filtering to redirect the device HTTP request to a local server if the terminal device does not utilize said protocol.

In a further embodiment of the apparatus, the access point includes a means to communicate IEEE 802.1x protocol exchanges and means to establish IP packet filtering through an IP filter module and state information for the HTTP server to control the terminal device access during and after IEEE 802.1x based authentication process if the access point detects that the terminal device is an IEEE 802.1x client.

## BRIEF DESCRIPTION OF THE DRAWINGS

The invention is best understood from the following detailed description when read in connection with the accompanying drawing. The various features of the drawings are not specified exhaustively. On the contrary, the various features may be arbitrarily expanded or reduced for clarity. Included in the drawing are the following figures:

FIG. 1 is a block diagram of a communications system for practicing the method of the present invention for improving the security of a terminal device in a WLAN environment.

FIG. 2 is a flow diagram of the method of the authentication sequence of present invention.

FIG. 3 is a flow diagram of the method of the present invention illustrating an authentication failure.

FIG. 4 is a block diagram of an apparatus for implementing the present invention.

## DETAILED DESCRIPTION OF THE INVENTION

In the figures to be discussed the circuits and associated blocks and arrows represent functions of the process according to the present invention, which may be implemented as electrical circuits and associated wires or data busses, that transport electrical signals. Alternatively, one or more associated arrows may represent communication (e.g., data flow) between software routines, particularly when the present method or apparatus of the present invention is implemented as a digital process.

In accordance with FIG. 1, one or more mobile terminals represented by $140_1$ through $140_n$ communicate through an access point (AP) through $130_n$, local computer 120, in association with firewalls 122 and one or more virtual operators $150_{1\text{-}n}$, such as authentication server $150_n$. Communication from terminals $140_{1\text{-}n}$ typically require accessing a secured data base or other resources, utilizing the Internet 110 and associated communication paths 154 and 152 that require a high degree of security from unauthorized entities, such as would be hackers.

As further illustrated in FIG. 1, the WLAN architecture encompasses several components and services that interact to provide station mobility transparent to the higher layers of a network stack. The AP stations such as access points $130_{1\text{-}n}$ and mobile terminals $140_{1\text{-}n}$ as the components connect to the wireless medium and typically contain the functionality of the IEEE 802.1x protocols, that being MAC (Medium Access Control) $134_{1\text{-}n}$, and corresponding PHY (Physical Layer) (unshown), and a connection 127 to the wireless media. Communication functions and protocols are implemented in the hardware and software of a wireless modem or a network access or interface card. This invention proposes a method for implementing a means in the communication stream such that an access point $130_n$ improves the security of a terminal device in a WLAN environment 115 whether the device utilizes an IEEE 802.1x protocol or not and remain within the compatibility requirements of a IEEE 802.1x WLAN MAC layers for downlink traffic (e.g. from the an authentication server 150 to the mobile terminal $140_n$ such as a laptop) as each may participate in the authentication

of one or more wireless mobile devices $140_{1-n,}$, a local server 120 and a virtual operator such as the authentication server 150.

In accordance with the present principles of the invention, an access 160 enables each mobile terminals $140_{1-n,}$ to securely access a WLAN 115 by authenticating the mobile terminal $140_{1-n}$ as well as its communication stream in accordance with the IEEE 802.1x protocol or other optional protocol as the specific terminal $140_{1-n}$ may choose. The manner in which the access 160 enables such secure access can best be understood by reference to FIG. 2, which depicts the sequence of interactions that occurs among a mobile wireless communication device, say mobile terminal $140_{n,}$ the public WLAN 115, Authentication server $150_n$. When configured with the IEEE 802.1 x protocols, the access point $130_n$ of FIG. 1 maintains a controlled port and an un-controlled port, through which the access point exchanges information, with the mobile terminals $140_n$. The controlled port maintained by the access point $130_n$ serves as the entryway for non-authentication information, such as data traffic, to pass through the access point between the WLAN 115 and the mobile terminals $140_n$. Ordinarily, the access point $130_{-n}$ keeps the respective controlled port closed in accordance with the IEEE 802.1x protocol until authentication of the mobile wireless communications device. The access points $130_n$ always maintains the respective uncontrolled port open to permit the mobile terminals $140_n$ to exchange authentication data with the local survey or virtual server $150_n$.

With reference to FIG. 2, a further embodiment of the present invention is the utilization of the access point $130_n$ to create several operational states. Following an EAP Response-Identity packet 220 a state 1x_progress 340 indicates that the mobile terminal $140_n$ is an IEEE 802.1x client and the 802.1x authentication process is ongoing. Such means to select from one or more available security protocols is well known by those skilled in the art of programming and engineering in a WLAN environment. The 802.1X engine 325 is therefore responsible for client detection and providing the client capability information to other modules of the system. In addition it also implements RADIUS client functionality to convert EAP messages to RADIUS messages, forwarding such messages in the form of an radius access request 230 and responding to radius access reject messages 240. The packet filter module 330 is responsible for filtering packets based on the criteria set by other modules. The method utilized by the access point to determines that the terminal is not IEEE

802.1x protocol compliant is based upon timing out a pre-established timer, before it receives the EAP request identity response packet.

More particularly, FIG. 3 illustrates an embodiment of the method of the present invention wherein the access point $130_n$ detects that the mobile terminal $140_n$ is not an authenticated IEEE 802.1x client, and redirects client 335 to thereby configure through an IP packet filter module 330 a redirect to the HTTP server 120 via a web request redirect 345. Alternatively, mobile terminal $140_n$ may send a direct web access request 355, which is redirected by the packet filter module 330 to the HTTP server 120. The HTTP server 120 responds with information 350 specifically related to the browser based authentication.

In the case where the access point $130_n$ detects that the terminal device is an IEEE 802.1x client, it permits normal IEEE 802.1x protocol communication exchanges to proceed through the access point $130_n$ and sets up appropriate IP packet filtering through IP filter module 330 and state information for the HTTP server 120 to control the mobile terminal $140_n$ user access during and after IEEE 802.1x based authentication process.

As indicated above, the WLAN 115 system must maintain proper state information for the system to function properly. Such state information will be provided by the access point $130_n$ 802.1x engine, which is used by, among other things, the packet filtering function 330 and the HTTP server 120. With reference to FIG. 3, a further embodiment of the present invention is the utilization of the access point $130_n$ 802.1 x engine to create several operational states. Following a Response-Identity EAP packet 220 a state 1x_progress 340 indicates that the mobile terminal $140_n$ is an IEEE 802.1x client and the 802.1x authentication process is ongoing. Following a Response-Identity EAP packet 220 a state 1x_failure 350 would indicate that the 802.1x authentication process failed for one of more reasons, not pertinent to the invention herein. Following a Response-Identity EAP packet 220 a state non_1x 360 would indicate that the mobile terminal $140_n$ is a non-IEEE 802.1x client. Because for such a client, all access controls are done at the higher layers, no further classification of state is necessary.

The access point includes an 802.1X engine 325, which is a module that implements the IEEE 802.1X protocol with the determining means necessary to carry out the steps of the invention. Such means to select from one or more available security protocols is well known by those skilled in the art of programming and engineering in a WLAN environment. The

802.1X engine 325 is therefore responsible for client detection and providing the client capability information to other modules of the system. In addition it also implements RADIUS client functionality to convert EAP messages to RADIUS messages. The packet filter module 330 is responsible for filtering packets based on the criteria set by other modules.

Referring to FIG. 4 is an apparatus of the present the invention for improving the security of the terminal device $140_n$ in the WLAN 115 environment. The access point $130_n$ maintains communication with the terminal device $140_n$ terminal device and utilizes a means 415 to determine whether the terminal device $140_n$ utilizes an IEEE 802.1x protocol and if the terminal $140_n$ does not utilize said protocol then the access point $130_n$ employs an authentication means 420 compatible with the terminal device $140_n$ otherwise the access point employs an IEEE 802.1x protocol utilizing means 425. The access point $130_n$ means to determine includes communicating to the terminal device $140_n$ a Request-Identity EAP packet and if the mobile terminal $140_n$ utilizes the IEEE 802.1x protocol the access point $130_n$ receives a Response-Identity EAP packet. The access point $130_n$ further comprises the means 430 to configure an IP packet filtering to redirect through means 435 the device HTTP request to a local server if the terminal device $140_n$ does not utilize the protocol. In the event the IEEE 802.1x protocol is utilized then the means 425 utilizes means 440 to insure that the communication is not redirected.

In a further embodiment of the apparatus, the access point includes a means to communicate IEEE 802.1x protocol exchanges and means to establish IP packet filtering through an IP filter module and state information for the HTTP server to control the terminal device access during and after IEEE 802.1x based authentication process if the access point detects that the terminal device is an IEEE 802.1x client.

It is to be understood that the form of this invention as shown is merely a preferred embodiment. Various changes may be made in the function and arrangement of parts; equivalent means may be substituted for those illustrated and described; and certain features may be used independently from others without departing from the spirit and scope of the invention as defined in the following claims.

1. A method for controlling access by a user terminal to a communications network, comprising the steps of:

receiving from the user terminal a request to access the communications network;

transmitting to the user terminal an identity request message;

receiving from the user terminal, if the user terminal utilizes a predetermined authentication protocol, a response to the identity request message;

determining whether the user terminal uses the predetermined authentication protocol in response to the response to the identity request message; and

selecting an authentication mechanism, compatible with the user terminal in response to the determination, for allowing user terminal access to the communications.

2. The method according to claim 1, wherein the user terminal comprises a mobile terminal and the communications network comprises a wireless local area network WLAN that complies with the IEEE 802.11 standards.

3. The method according to claim 2, wherein the selecting step includes selecting an appropriate authentication server coupled to the WLAN in response to the determination.

4. A method for controlling mobile terminal access to a wireless local area network (WLAN), comprising the steps of:

receiving from the mobile terminal a request to access the WLAN;

transmitting to the mobile terminal an identity request message;

receiving from the mobile terminal, if the mobile terminal utilizes an IEEE 802.1x protocol, a response to the identity request message;

determining whether the mobile terminal is IEEE 802.1x compliant in response to the response to the identity request message; and

selecting an authentication mechanism, compatible with the mobile terminal in response to the determination, for allowing mobile terminal access to the WLAN.

5. The method according to claim 4, further comprising the steps of, if the mobile terminal is IEEE 802.1x compliant, transmitting an authentication request to an authentication server and receiving an authentication response utilizing the IEEE 802.1x protocol, and controlling mobile terminal access to the WLAN in response to the authentication response.

6. The method according to claim 4, further comprising the steps of, if the mobile terminal is not IEEE 802.1x compliant, redirecting an authentication request to an HTTP server for utilizing a browser based authentication.

7. The method according to claim 6, further comprising the step of configuring a packet filtering module to redirect the authentication request to the HTTP server.

8. The method according to claim 7, further comprising the step of maintaining state information in the WLAN for use by the packet filtering module and the HTTP server.

9. The method according to claim 8, wherein the state information includes one of a first state indicative of ongoing authentication process, a second state indicative of authentication failure, a third state indicative of authentication success, and a fourth state indicative of a non IEEE 802.1x mobile terminal.

10. An access point in communication with a terminal device in a wireless local area network, comprising:

a means to determine whether the terminal device utilizes an IEEE 802.1x protocol and, if the terminal does not utilize said protocol, then the access point employing an authentication means compatible with the terminal device otherwise the access point employing an IEEE 802.1x protocol.

11. The access point in claim 10, wherein the means to determine includes communicating to the terminal device a Request-Identity EAP packet and if the mobile terminal utilizes the IEEE 802.1x protocol the access receives a Response-Identity EAP packet.

12. The access point in claim 11, further comprises the means to configure an IP packet filtering to redirect the device HTTP request to a local server if the terminal device does not utilize said protocol.

13. The access point in claim 10, further comprises means to communicate IEEE 802.1x protocol exchanges and means to establish IP packet filtering through an IP filter module and

state information for the HTTP server to control the terminal device access during and after IEEE 802.1x based authentication process if the access point detects that the terminal device is an IEEE 802.1x client.

14. A method for controlling access by a terminal device in a wireless local area network by determining whether the terminal device utilizes an IEEE 802.1x protocol comprising the steps of:

an access point communicating to the mobile terminal a request to identify, and if the terminal device utilizes an IEEE 802.1x protocol, acknowledging the request to identify, otherwise the access point determining that the terminal is not IEEE 802.1x compliant and selecting an authentication mechanism compatible with the mobile terminal.

15. The method according to claim 14, wherein the access point determines that the terminal is not IEEE 802.1x compliant when it does not receive an EAP identity response packet after a timeout value.

16. The method according to claim 15, further comprising the step of access point detecting that if the terminal device is not IEEE 802.1x compliant, then configuring an IP packet filter and redirecting a user HTTP request to a local server.

17. The method according to claim 16, further comprising the step of the local server communicating to the terminal device information specifically related to a browser based authentication.

18. The method according to claim 17, further comprising the step of the access point transitioning to a state if the terminal device utilizes the IEEE 802.1x protocol that indicates that the terminal device is IEEE 802.1x compliant and thereafter processing all communication utilizing the IEEE 802.1x protocol.

19. The method according to claim 17, further comprising the step of the access point transitioning to a state corresponding to browser based authentication if the authentication process fails.

20. The method according to claim 14, further comprising the step of the access point transitioning to a state corresponding to browser based authentication if the terminal device is not IEEE 802.1x compliant.

21. A method for controlling access of a terminal device in a WLAN by determining whether the terminal device utilizes an IEEE 802.1x protocol comprising the steps of: communicating through the an access point to the mobile terminal a request to identify, and if the terminal device utilizes an IEEE 802.1x protocol, acknowledging the request to identify, otherwise determining by the access point that the terminal is not IEEE 802.1x compliant and selecting an authentication mechanism compatible with the terminal.

22. The method according to claim 21, further comprising the step of determining in the access point that terminal is not IEEE 802.1x compliant if it does not receive an EAP identity response packet after a preset time.

23. The method according to claim 21, further comprising the step of detecting in the access point that if the terminal device is not IEEE 802.1x compliant, then configuring an IP packet filter and redirecting a user HTTP request to a local server.

24. The method according to claim 23, further comprising the step of communicating from the local server to the terminal device, information specifically related to a browser based authentication.

25. The method according to claim 21, further comprising the step of transitioning to a state in the access point if the terminal device utilizes the IEEE 802.1x protocol that indicates that the terminal device is IEEE 802.1x compliant and thereafter processing all communication utilizing the IEEE 802.1x protocol.

26. The method according to claim 25, further comprising the step of transitioning to a state in the access point corresponding to browser based authentication if the authentication process fails.

27. The method according to claim 21, further comprising the step of transitioning to a state in the access point corresponding to browser based authentication if the terminal device is not IEEE 802.1x compliant.

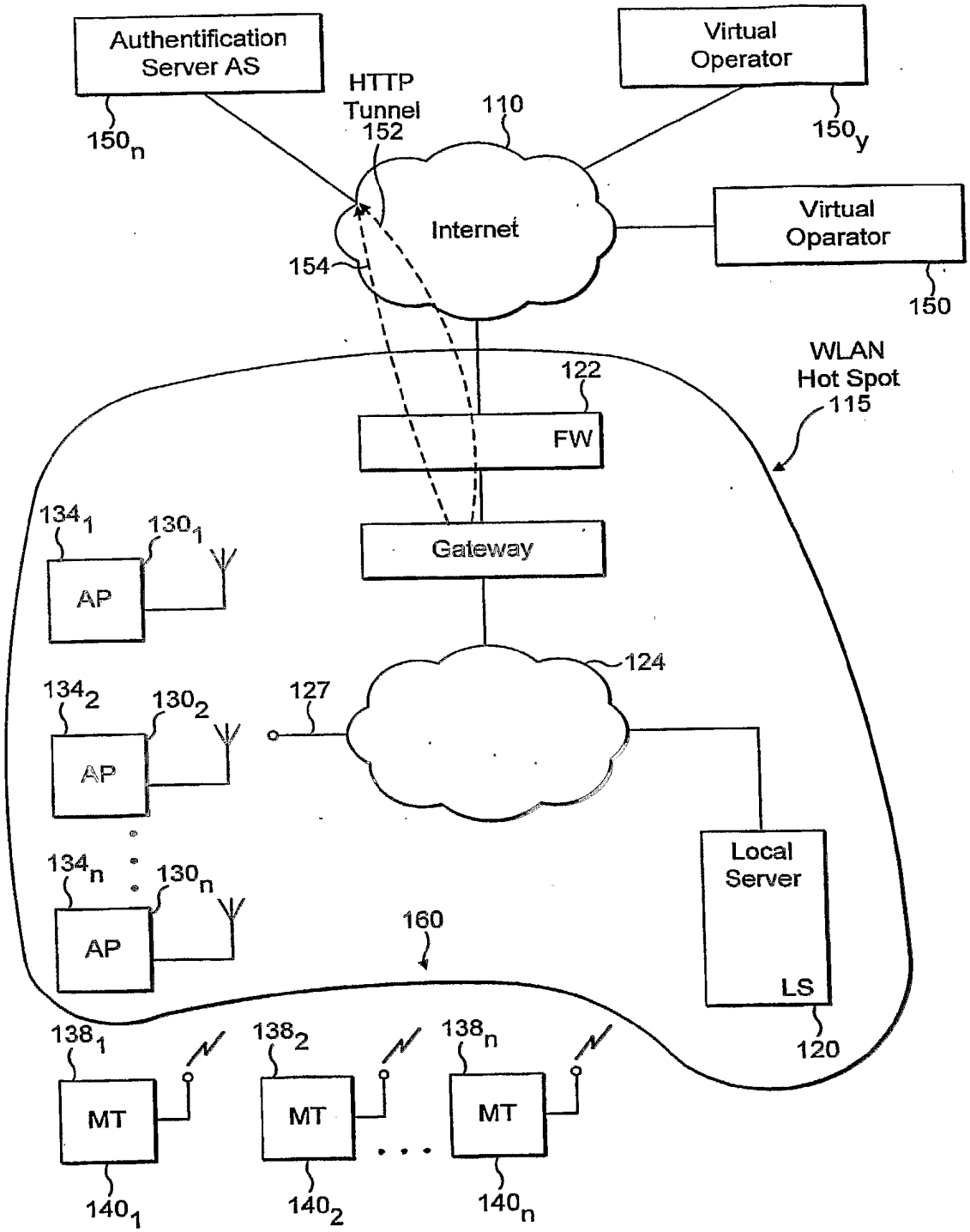

Authentification Server AS
150n
HTTP Tunnel
152
110
Virtual Operator
150y
Internet
154
Virtual Oparator
150
WLAN Hot Spot
115
122
FW
Gateway
124
127
134 1
130 1
AP
134 2
130 2
AP
134 n
130 n
AP
160
Local Server
LS
120
138 1
138 2
138 n
MT
MT
MT
140 1
140 2
140 n

FIG. 1

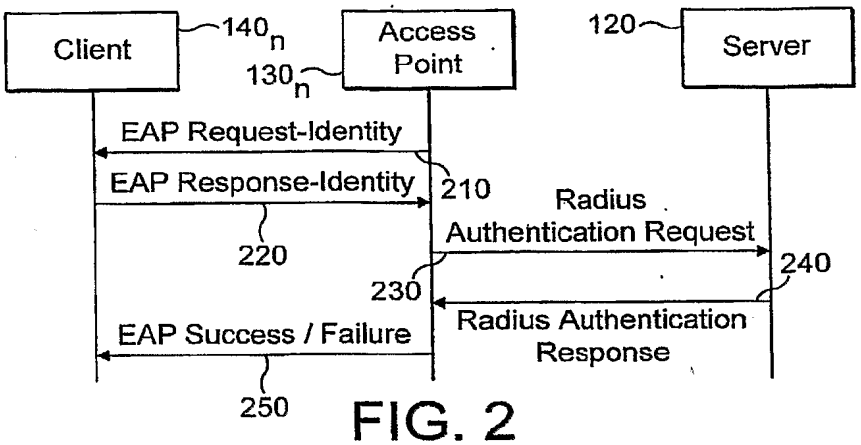

Client
140n
Access Point
130n
120
Server
EAP Request-Identity
EAP Response-Identity
210
220
Radius Authentication Request
240
230
Radius Authentication Response
EAP Success / Failure
250

FIG. 2

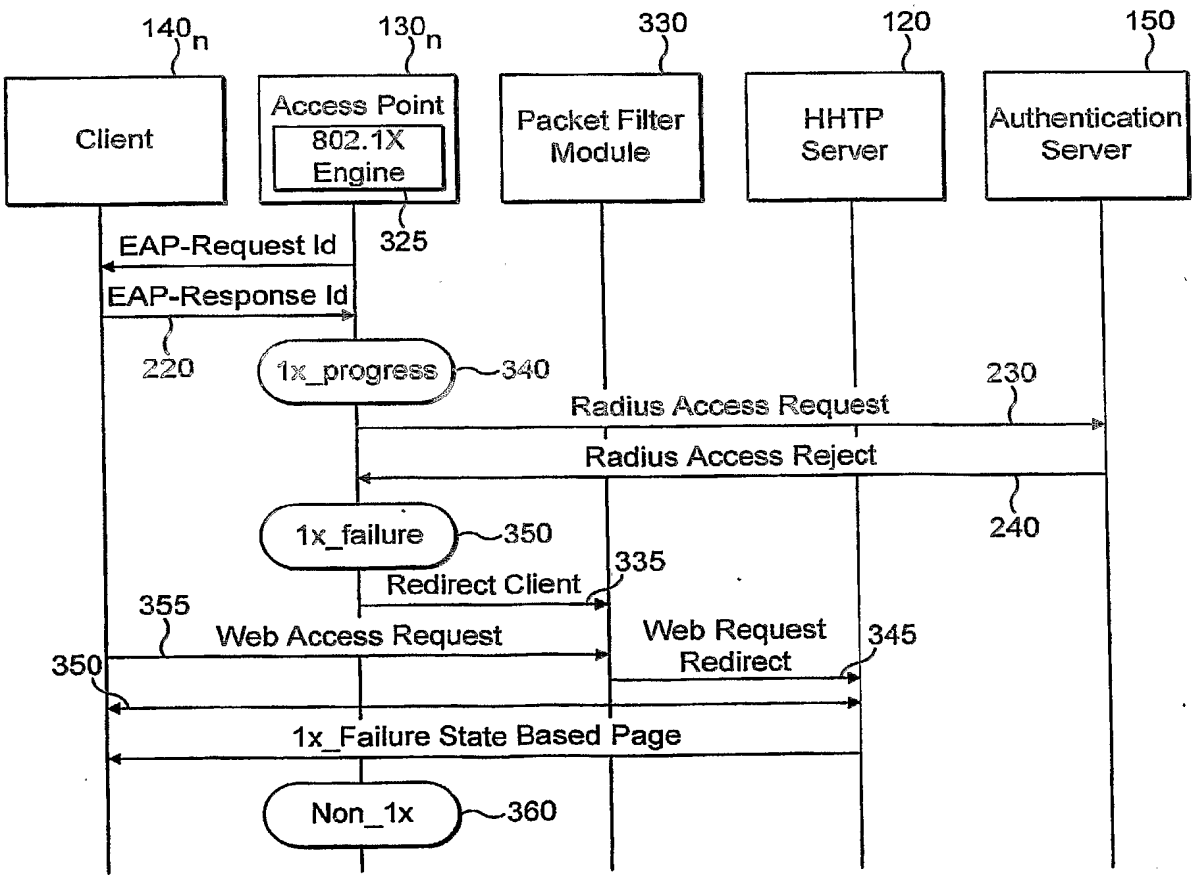

140n
130n
330
120
150
Client
Access Point
802.1X Engine
Packet Filter Module
HHTP Server
Authentication Server
325
EAP-Request Id
EAP-Response Id
220
1x_progress
340
230
Radius Access Request
Radius Access Reject
240
1x_failure
350
335
Redirect Client
355
Web Access Request
Web Request Redirect
345
350
1x_Failure State Based Page
Non_1x
360

FIG. 3

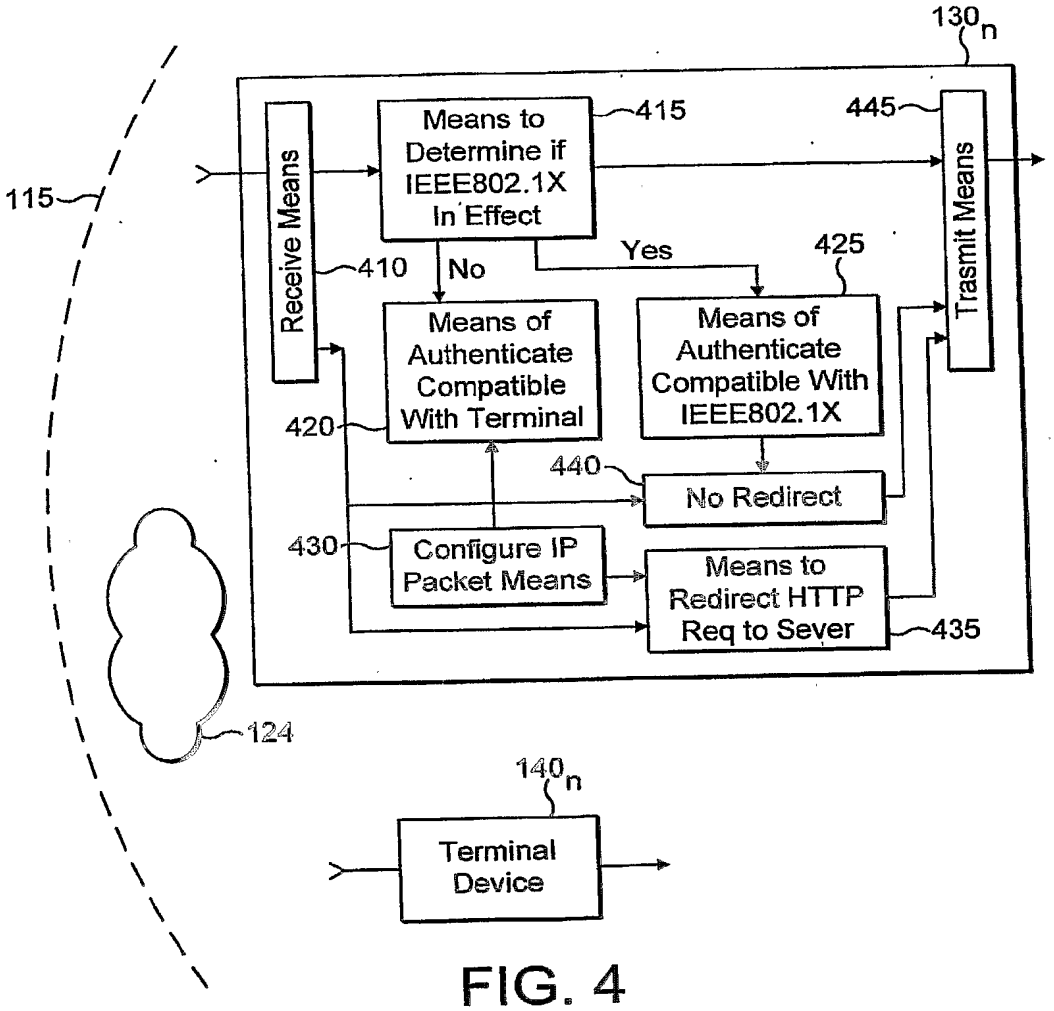

130n
115
Receive Means
Means to Determine if IEEE802.1X In Effect
415
445
Trasmit Means
410
No
Yes
425
Means of Authenticate Compatible With Terminal
420
Means of Authenticate Compatible With IEEE802.1X
440
No Redirect
430
Configure IP Packet Means
Means to Redirect HTTP Req to Sever
435
124
140n
Terminal Device

FIG. 4